DDP Enterprise Server - Virtual Edition

Quick Start Guide
and
Installation Guide

© 2014 Dell Inc.

Registered trademarks and trademarks used in the DDP|E, DDP|ST, and DDP|CE suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen Tec® and Eikon® are registered trademarks of Authen Tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. Dropbox℠ is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App Store℠, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®℠, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecurID® are registered trademarks of EMC Corporation. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc.

This product uses parts of the 7-Zip program. The source code can be found at www.7-zip.org. Licensing is under the GNU LGPL license + unRAR restrictions (www.7-zip.org/license.txt).

Virtual Edition uses third-party libraries from "urwid" under the terms of GNU Lesser General Public License. The copyright notice and GNU Lesser General Public License can be found in the AdminHelp on the Attributions, Copyrights, and Trademarks page.

2014-10

Protected by one or more U.S. Patents, including: Number 7665125; Number 7437752; and Number 7665118.

Information in this document is subject to change without notice.

Contents

1 Quick Start Guide 5

2 Installation Guide 9

About DDP Enterprise Server - VE **9**

Customer Support **9**

Requirements **10**

Install DDP Enterprise Server - VE **13**

Install VE Remote Management Console **14**

Install and Configure Proxy Mode **14**

VE Terminal - Basic Configuration Tasks **15**

Change Hostname 15

Change Network Settings 15

Set DMZ Hostname 15

Change Time Zone 16

Update DDP Enterprise Server - VE 16

Change User Passwords 16

Set up File Transfer (FTP) Users 17

Enable SSH 17

Start or Stop VE Servers 17

Reboot VE 17

Shut down VE 18

VE Terminal - Advanced Configuration Tasks **18**

Set or Change the Database Password 18

Configure SMTP Settings 18

Import an Existing Certificate or Enroll a New Server Certificate 19

Configure Log Rotation 20

Backup and Restore 20

Enable Database Remote Access 21

Enable DMZ Server Support 21

DDP Enterprise Server - VE Administrator Tasks **21**

Set or Change DDP Enterprise Server - VE Terminal Language 21

Check Server Status 21

View Logs 22

Open the Command-line Interface 22
Generate a System Snapshot Log. 23

DDP Enterprise Server - VE Maintenance 23

DDP Enterprise Server - VE Troubleshooting 23

Post-Installation Configuration Tasks 23
Configure VE for Dell Data Protection | Cloud Edition. 23
Install and Configure EAS Management for Dell Data Protection | Mobile Edition 23
Enable Manager Trust Chain Check. 25

VE Remote Management Console Administrator Tasks 25
Assign Dell Administrator Role 25
Log in with Dell Administrator Role 26

Quick Start Guide

This Quick Start Guide is for more experienced users, to get DDP Enterprise Server - VE up and running fast. As a general rule, Dell recommends installing the DDP Enterprise Server - VE first, followed by installation of clients.

For more detailed instructions, see the Installation Guide on page 9.

For information on how to update an existing DDP Enterprise Server - VE, see Update DDP Enterprise Server - VE on page 16.

DDP Enterprise Server - VE Prerequisites

A complete list of Requirements can be found on page 10.

Hardware

The recommended disk space for DDP Enterprise Server - VE is 80 GB.

Virtualized Environment

DDP Enterprise Server - VE v8.5 has been validated with the following virtualized environments.

Virtualized Environments
• VMWare Workstation 9 — 64-bit CPU required — 4 GB RAM recommended — See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems — Hardware must conform to minimum VMWare requirements — 4 GB minimum RAM for dedicated image resource — See http://pubs.vmware.com/workstation-9/index.jsp for more information
• VMWare Workstation 10 — 64-bit CPU required — 4 GB RAM recommended — See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems — Hardware must conform to minimum VMWare requirements — 4 GB minimum RAM for dedicated image resource — See http://pubs.vmware.com/workstation-10/index.jsp for more information
• VMWare ESXi 5.5 — 64-bit x86 CPU required — Host computer computer with at least two cores — 8 GB RAM minimum recommended — An Operating System is not required — See http://www.vmware.com/resources/compatibility/search.php for a complete list of supported Host Operating Systems — Hardware must conform to minimum VMWare requirements — 8 GB minimum RAM for dedicated image resource — See http://pubs.vmware.com/vsphere-55/index.jsp for more information

Install DDP Enterprise Server - VE

1. Browse to the directory where the Dell Data Protection files are stored and double-click to import into VMWare **DDP Enterprise Server - VE v8.x.x Build x.ova**.
2. Power on DDP Enterprise Server - VE.
3. Follow the on-screen instructions.

Configuration

Before you activate users, you must complete the following Configuration tasks at the DDP Enterprise Server - VE Terminal:

- Set or Change the Database Password on page 18
- Configure SMTP Settings on page 18
- Import an Existing Certificate or Enroll a New Server Certificate on page 19
- Update DDP Enterprise Server - VE on page 16
- Install an FTP client that supports SFTP on port 22, and Set up File Transfer (FTP) Users on page 17.

NOTE: If your Enterprise Edition clients will be entitled from the factory or you purchase licenses from the factory, set the GPO on the domain controller to enable entitlements (this may not be the same server running Enterprise Edition). Ensure that outbound port 443 is available to communicate with the Server. If port 443 is blocked (for any reason), the entitlement functionality will not work.

Install VE Remote Management Console

1. Copy the Server Remote Console Installer package from the Dell Data Protection installation media to the local computer that will access the DDP Enterprise Server - VE.
2. Double-click **setup.exe** to launch the installer.
3. Follow the on-screen instructions.
4. When finished, log in to the VE Remote Management Console using the default credentials **superadmin/changeit**.

If your organization has external facing devices, see Install and Configure Proxy Mode on page 14.

Administrative Tasks

If you have not launched the VE Remote Management Console, do so now. The default credentials are **superadmin/changeit**.

Dell recommends that you assign administrator roles as soon as it is convenient. To complete this task now, see Assign Dell Administrator Role on page 25.

Click "?" in the upper right corner of the VE Remote Management Console to launch the Administrator Help. The *Get Started* page displays. Follow the instructions to add a domain.

Baseline polices have been set for your organization but may need to be modified depending on your specific needs, as follows (licensing and entitlements guide all activations):

- Windows computers with Hardware Crypto Accelerators will be encrypted
- Windows computers will be encrypted
- Computers with self-encrypting drives will be encrypted
- External media will not be encrypted
- Devices connected to ports will not be encrypted

- BitLocker management is not enabled
- Cloud Edition is not enabled
- Mobile Edition is not enabled

See the Administrator Help topic “Manage Policies” to learn how to work with policies.

Quick Start tasks are complete.

Installation Guide

This Installation Guide is for less experienced users, to install and configure DDP Enterprise Server - VE. As a general rule, Dell recommends installing the DDP Enterprise Server - VE first, followed by installation of clients.

For information on how to update an existing DDP Enterprise Server - VE, see Update DDP Enterprise Server - VE on page 16.

About DDP Enterprise Server - VE

The DDP Enterprise Server - VE is the security administration piece of Dell's solution. The VE Remote Management Console allows administrators to monitor the state of endpoints, policy enforcement, and protection across the enterprise. Proxy Mode provides a front-end DMZ Mode option for use with DDP Enterprise Server - VE.

DDP Enterprise Server - VE has the following features:

- Centralized management of up to 3,500 devices
- Role-based security policy creation and management
- Administrator-assisted device recovery
- Separation of administrative duties
- Automatic distribution of security policies
- Trusted paths for communication between components
- Unique encryption key generation and automatic secure key escrow
- Centralized compliance auditing and reporting
- Auto-generation of self-signed certificates

Customer Support

When contacting Dell Pro Support, have the following information available:

- The version number and build date of the VE Remote Management Console can be found in the **About** link in the VE Remote Management Console.
- The version and build numbers of DDP Enterprise Server - Virtual Edition can be found at the top of the VE Terminal Main Menu.
- Operating system version for the server/workstation where the relevant components are running.
- A detailed description of the issue you are experiencing.
- Information about how we can reach you.

Requirements

DDP Enterprise Server - VE Prerequisites

Hardware

The recommended disk space for DDP Enterprise Server - VE is 80 GB.

Virtualized Environment

DDP Enterprise Server - VE v8.5 has been validated with the following virtualized environments.

Virtualized Environments
• VMWare Workstation 9 — 64-bit CPU required — 4 GB RAM recommended — See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems — Hardware must conform to minimum VMWare requirements — 4 GB minimum RAM for dedicated image resource — See http://pubs.vmware.com/workstation-9/index.jsp for more information
• VMWare Workstation 10 — 64-bit CPU required — 4 GB RAM recommended — See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems — Hardware must conform to minimum VMWare requirements — 4 GB minimum RAM for dedicated image resource — See http://pubs.vmware.com/workstation-10/index.jsp for more information
• VMWare ESXi 5.5 — 64-bit x86 CPU required — Host computer computer with at least two cores — 8 GB RAM minimum recommended — An Operating System is not required — See http://www.vmware.com/resources/compatibility/search.php for a complete list of supported Host Operating Systems — Hardware must conform to minimum VMWare requirements — 8 GB minimum RAM for dedicated image resource — See http://pubs.vmware.com/vsphere-55/index.jsp for more information

VE Remote Management Console Prerequisites

The following table details the software that must be in place before installing VE Remote Management Console.

Prerequisites
• Windows Installer 3.1 or later Windows Installer 3.1 or later must be installed on the server where the installation is taking place.
• Microsoft .NET Framework Version 4.0 •Microsoft has published security updates for .NET Framework Version 4.

Hardware

The following table details the *minimum* hardware requirements for VE Remote Management Console.

Processor
2 GHz Core 2 Duo or better
RAM
+-2 GB, depending on configuration
Free Disk Space
+-250 MB free disk space (plus virtual paging space)
Network Card
10/100/1000 network interface card
Miscellaneous
TCP/IP installed and activated

Software

The following table details the software requirements for the VE Remote Management Console.

NOTE: Always disable UAC when using Windows Server 2008. After disabling UAC, the server **must** be rebooted for this change to take effect.

Registry location for Windows Servers: HKLM\SOFTWARE\Dell.

Operating System
• Windows Server 2003 SP2 32-bit or 64-bit – Standard Edition – Enterprise Edition
• Windows Server 2003 R2 and R2 SP2 32-bit or 64-bit – Standard Edition – Enterprise Edition
• Windows Server 2008 R2 SP0-SP1 64-bit – Standard Edition – Enterprise Edition
• Windows Server 2008 SP2 32-bit or 64-bit – Standard Edition – Enterprise Edition
• Microsoft Windows 7 SP0-SP1 – Enterprise – Professional – Ultimate

Proxy Mode Prerequisites

The following table details the software that must be in place before installing Proxy Mode.

Prerequisites
• Windows Installer 3.1 or later Windows Installer 3.1 or later must be installed on the server where the installation is taking place.
• Microsoft Visual C++ 2010 Redistributable Package If not installed, the installer will install it for you.
• Microsoft .NET Framework Version 3.5 SP1
• Microsoft .NET Framework Version 4.0 Microsoft has published security updates for .NET Framework Version 4.
• Microsoft Windows Identity Foundation

Hardware

The following table details the *minimum* hardware requirements for Proxy Mode.

Processor
2 GHz Core 2 Duo or better
RAM
+-2 GB minimum dedicated RAM / 4 GB dedicated RAM recommended
Free Disk Space
+-1.5 GB free disk space (plus virtual paging space)
Network Card
10/100/1000 network interface card
Miscellaneous
TCP/IP installed and activated

Software

The following table details the software requirements for the Proxy Mode server.

NOTE: Always disable UAC when using Windows Server 2008. After disabling UAC, the server **must** be rebooted for this change to take effect.

Registry location for Windows Servers: HKLM\SOFTWARE\Dell.

Operating System
• Windows Server 2003 SP2 32-bit or 64-bit – Standard Edition – Enterprise Edition
• Windows Server 2003 R2 and R2 SP2 32-bit or 64-bit – Standard Edition – Enterprise Edition
• Windows Server 2008 R2 SP0-SP1 64-bit – Standard Edition – Enterprise Edition
• Windows Server 2008 SP2 32-bit or 64-bit – Standard Edition – Enterprise Edition

Install DDP Enterprise Server - VE

Before you begin, ensure that all system and virtual environment Requirements are met.

1. Locate the Dell Data Protection files in the installation media and double-click to import into VMWare **DDP Enterprise Server - VE v8.x.x Build x.ova**.
2. Power on DDP Enterprise Server - VE.
3. Select the language for the license agreement, and select **Display EULA**.
4. Read the agreement, and select **Accept EULA**.
5. If an update is available, select **Accept**.
6. At the default password change prompt, select **Yes**.
7. In the *Set ddpuser Password* screen, enter the current (default) password, **ddpuser**, then enter a unique password, re-enter the unique password, and select **OK**.
8. In the *Configure Hostname* dialog, use the Backspace key to remove the default hostname. Enter a unique hostname and select **OK**.

9 In the *Configure Network Settings* dialog, choose either option below, then select **OK**.

— (Default) Use DHCP.

— (Recommended) In the Use DHCP field, press the Spacebar to remove the X and manually enter these addresses, as applicable:
Static IP
Network Mask
Default Gateway
DNS Server 1
DNS Server 2
DNS Server 3

NOTE: When using a static IP, you must also create a host entry in the DNS server.

10 In the *Time Zone* screen, use the arrow keys to highlight your time zone and select **Enter**.

11 At the time zone confirmation prompt, select **OK**.

12 When the message displays to indicate that initial configuration is completed, select **OK**.

13 Set or Change the Database Password as explained on page 18.

14 Configure SMTP Settings as explained on page 18.

15 Import an Existing Certificate or Enroll a New Server Certificate as explained on page 19.

16 Update DDP Enterprise Server - VE as explained on page 16.

17 Install an FTP client that supports SFTP on port 22, and Set up File Transfer (FTP) Users as explained on page 17.

DDP Enterprise Server - VE installation tasks are complete.

Install VE Remote Management Console

1 Copy the Server Remote Console Installer package from the Dell Data Protection installation media to the local computer that will access the DDP Enterprise Server - VE.

2 Double-click **setup.exe** to launch the installer.

3 Select the language for the installation and click **OK**.

4 Read and accept the Dell End User License Agreement and click **Next**.

5 Confirm or **Change** the installation folder and click **Next**.

6 Enter the hostname or IP address of the DDP Enterprise Server - VE and click **Next**.

7 To begin the installation, click **Install**.

8 When the installation is complete, click **Finish**.

9 When finished, log in to the VE Remote Management Console using the default credentials **superadmin/changeit**.

Install and Configure Proxy Mode

Proxy Mode provides a front-end (DMZ Mode) option for use with DDP Enterprise Server - VE. If you want to install Proxy Mode, follow these instructions.

To perform this installation, you will need the fully-qualified hostname of the DMZ server.

1 Copy the Proxy Mode Installer package from the Dell Data Protection installation media to the DMZ server.

2 Double-click **setup.exe** to launch the installer.

3 Select the language for the installation and click **OK**.

4 Read and accept the Dell End User License Agreement, and click **Next**.

5 Enter the fully qualified domain name of the proxy server.

6 Select either to import an existing certificate or create and import a self-signed certificate, and click **Next**.

— *Import an existing certificate* - Provide the path to the certificate and password.

— *Create a self-signed certificate and import it to key store* - Provide the fully qualified domain name of the proxy server and information about your organization.

7 To begin installation, click **Install**.

8 When installation is complete, click **Finish**.

9 When finished, select **All Programs > Dell > Enterprise Edition > Policy Proxy > Start Dell Policy Proxy Service**.

NOTE: To use Proxy Mode, you must also Set DMZ Hostname and Enable DMZ Server Support.

VE Terminal - Basic Configuration Tasks

Basic configuration tasks are accessed from the Main Menu.

Change Hostname

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

1 From the *Basic Configuration* menu, select **Hostname**.

2 Use the Backspace key to remove the existing DDP Enterprise Server - VE hostname then replace it with a new hostname and select **OK**.

Change Network Settings

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

1 From the *Basic Configuration* menu, select **Network Settings**.

2 In the *Configure Network Settings* screen, choose either option below then select **OK**.

— (Default) Use DHCP.

— (Recommended) In the Use DHCP field, press the Spacebar to remove the X and manually enter these addresses, as applicable:
Static IP
Network Mask
Default Gateway
DNS Server 1
DNS Server 2
DNS Server 3

NOTE: When using a static IP, you must create a host entry in the DNS server.

Set DMZ Hostname

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

1 From the *Basic Configuration* menu, select **DMZ Hostname**.

2 Enter the fully qualified domain name of the DMZ server and select **OK**.

NOTE: To use Proxy Mode (DMZ Mode), you must Install and Configure Proxy Mode.

Change Time Zone

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

1. From the *Basic Configuration* menu, select **Time Zone**.
2. In the *Time Zone* screen, use the arrow keys to highlight your time zone and select **Enter**.
3. At the time zone confirmation prompt, select **OK**.

Update DDP Enterprise Server - VE

This task should be performed after initial installation of DDP Enterprise Server - VE and also before clients are activated. To receive email notifications when VE updates are available, Configure SMTP Settings.

For information about an update see Release-Notes, located on the VE secure FTP server.

1. From the *Basic Configuration* menu, select **Update DDP Enterprise Server - VE**.
2. Select the desired action:
   - Set Update Server - Select this option to set or change the server location of DDP Enterprise Server - VE update packages.
     In the *Set Update Server* screen, use the Backspace key to remove the existing Server Hostname or IP address. Enter the new fully qualified domain name or IP address and select **OK**.

   NOTE: To update from an FTP site, enter the FTP user name and password, followed by the URL.

   - Check for Update - Select this option to check the Update Server for a DDP Enterprise Server - VE update package.
   - Download Update - Select this option to download an update after it is discovered by Check for Update.
   - Apply Update - Select this option if you want to apply a DDP Enterprise Server - VE update package that you have downloaded.
     In the *Select an Update (.deb) File* screen, select the update package you want to install and press **Enter**.
   - Last successful update applied - Select this option to see the number and installation date of the current VE version.
3. Download and install the latest VE Remote Management Console.

   To access the VE Remote Management Console installer, follow these steps:

   a. From the VE FTP, locate the Server-Remote-Installer folder.

   b. Set up the FTP user to allow access to download the VE Remote Management Console installer (ServerRemoteConsoleInstaller-8.x.x) from the VE Server.

   c. Download the **ServerRemoteConsoleInstaller-8.x.x** zipped archive to the computer where the VE Remote Management Console will be installed, and extract the archived files.

   d. To install the VE Remote Management Console, run the appropriate **setup.exe** (x64 or x86) for the OS installed on that computer.

Change User Passwords

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

You can change passwords for these users:

- ddpuser - DDP Enterprise Server - VE Terminal Administrator
- ddpsupport - Dell Pro Support Administrator
- ddpconsole - DDP Enterprise Server - VE shell access

1. From the *Basic Configuration* menu, select **Change User Passwords**.

2 In the *Change User Passwords* screen, select user password to change and select **Enter.**

3 In the *Set Password* screen, enter the current password, enter the new password, re-enter the new password, and select **OK**.

Set up File Transfer (FTP) Users

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

You can give up to three users access to the secure FTP server of the DDP Enterprise Server - VE for backup and restore tasks. The VE FTP server can also be used to store or upload updates to DDP Enterprise Server - VE.

1 From the *Basic Configuration* menu, select **File Transfer (FTP) Users**.

2 In the *Configure FTP Users* screen, to enable an FTP User, press the Spacebar to enter an **X** in the Status field for the user.
To disable an FTP User, press the Spacebar to remove the **X** in the Status field for the user.

3 Enter a user name and password for the SFTP User.
Passwords must include the following:

— At least 8 characters

— At least 1 uppercase letter

— At least 1 digit

4 When you are finished entering SFTP users, select **OK**.

Enable SSH

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

You can enable SSH for the Support Administrator login, DDP Enterprise Server - VE shell access, and the VE Terminal command-line interface.

1 From the *Basic Configuration* menu, select **SSH Settings**.

2 Highlight the component for which you want to enable SSH, press the Spacebar to enter an **X** in its field, and select **OK**.

Start or Stop VE Servers

Perform this task only if needed. It is a best practice to restart the services any time a settings change is made.

1 To simultaneously start or stop all VE Servers, from the *Basic Configuration* menu, select either **Start Application** or **Stop Application**.

2 At the confirmation prompt, select **Yes**.

NOTE: Server state changes may require up to two minutes to complete.

Reboot VE

Perform this task only if needed.

1 From the *Basic Configuration* menu, select **Reboot Appliance**.

2 At the confirmation prompt, select **Yes**.

3 After restart, log in to DDP Enterprise Server - VE.

Shut down VE

Perform this task only if needed.

1. From the *Basic Configuration* menu, scroll down and select **Shutdown Appliance**.
2. At the confirmation prompt, select **Yes**.
3. After restart, log in to DDP Enterprise Server - VE.

VE Terminal - Advanced Configuration Tasks

Advanced configuration tasks are accessed from the Main Menu.

Set or Change the Database Password

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

1. From the *Advanced Configuration* menu, select **Database Password**.
2. Enter a password to access the database and select **OK**.

NOTE: Dell recommends that you back up passwords after installation is completed.

Configure SMTP Settings

To receive DDP Enterprise Server - VE email notifications **or** to use Dell Data Protection | Cloud Edition, follow the steps in this section to configure SMTP settings. DDP Enterprise Server - VE email notifications inform recipients of DDP Enterprise Server - VE server status error states, password updates, availability of DDP Enterprise Server - VE updates, and client license issues.

It is a best practice to restart the services any time a settings change is made.

To configure SMTP settings, follow these steps:

1. From the *Advanced Configuration* menu, select **Email Notifications**.
2. In the *Set up Email Notifications* screen, to enable email alerts, press the Spacebar to enter an **X** in the Enable Email Alerts field.
3. Enter the SMTP Server fully qualified domain name.
4. Enter the SMTP Port.
5. In the From User field, enter the email account ID that will send email notifications.
6. In the Enter User field, enter an email account ID for access to change configured email notifications.
7. In the Password field, enter a password for access to change configured email notifications.
8. In the Email list fields for VE Status, Password Updates, and Updates Availability, enter lists of recipients for each notification type.
   Follow these conventions when listing recipients:
   - Email address format is recipient@dell.com.
   - Recipients are separated with commas or semicolons.
9. Select **OK**.

Import an Existing Certificate or Enroll a New Server Certificate

Certificates must be in place before you can activate users against DDP Enterprise Server - VE.

You can import an existing certificate or create a certificate request through the DDP Enterprise Server - VE.

It is a best practice to restart the services any time a settings change is made.

Import an Existing Server Certificate

1. Export the existing certificate and its full chain of trust from its keystore.

   NOTE: Keep the export password because you will enter it when you import the certificate into DDP Enterprise Server - VE.
2. Store the certificate to the FTP Server of the DDP Enterprise Server - VE.
3. From the DDP Enterprise Server - VE *Advanced Configuration* menu, select **Server Certificates**.
4. Select **Import Existing Certificate**.
5. Select a certificate file to be installed on DDP Enterprise Server - VE.
6. When prompted, enter the certificate export password and select **OK**.
7. When the import is complete, select **OK**.

Enroll a New Server Certificate

1. From the *Advanced Configuration* menu, select **Server Certificates**.
2. Select **New Server Certificate**.
3. Select **Create Certificate Request.**
4. Complete the fields in the *Generate Certificate Request* screen:
   - *Two-letter country code.*
   - *State or province*: Enter the unabbreviated state or province name (example, Texas).
   - *Locality or city.* Enter the appropriate value (example, Dallas).
   - *Organization*: Enter the appropriate value (example, Dell).
   - *Organizational unit*: Enter the appropriate value (example, Security).
   - *Common name:* Enter the fully qualified domain name of the server where DDP Enterprise Server - VE is installed. This fully qualified name includes the hostname and the domain name (example, server.domain.com).
   - *Email ID:* Enter the email address to which your CSR will be sent.
5. Follow your organizational process for acquiring an SSL server certificate from a Certificate Authority. Send the contents of the CSR file for signing.
6. When you receive the signed certificate, export the certificate as a .p7b file, and download the full chain of trust in .der format.
7. Make backup copies of the certificate and chain of trust.
8. Upload the certificate file and its full chain of trust to the FTP Server of the DDP Enterprise Server - VE.
9. From the *Advanced Configuration* menu, select **Server Certificates**.
10. Select **New Server Certificate**.
11. Select **Complete Certificate Enrollment**.
12. Select the certificate file to be installed on DDP Enterprise Server - VE.
13. Enter the Certificate Password set when the Certificate Request was created.

To enable trust validation on Windows-based DDP|E encryption clients, see Enable Manager Trust Chain Check.

Configure Log Rotation

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

Daily log rotation is enabled by default. To change the default log rotation, from the *Advanced Configuration* menu, select **Logrotate Configuration**.

To disable log rotation, use the Spacebar to enter an **X** in the No rotation field and select **OK**.

To enable log rotation, follow these steps:

1. To enable daily, weekly, or monthly rotation, use the Spacebar to enter an **X** in the appropriate field.
   For weekly or monthly rotation, enter the appropriate day of the week or month as a numeral.
2. Enter a time for rotation in the Logrotate Time field.
3. Select **OK**.

Backup and Restore

Backups can be configured or performed at any time and are not required to begin using DDP Enterprise Server - VE.

Backups can be stored to an external secure FTP server (recommended) or to the DDP Enterprise Server - VE. If stored on the VE Server, when the disk is at 90 percent capacity, the oldest backups will be automatically deleted as new backups are stored.

NOTE: To preserve disk partition space and prevent automatic deletion of backups, remove unnecessary backups from DDP Enterprise Server - VE.

Backups are run daily, by default. Dell recommends storing backups to an external secure FTP server at a frequency that meets requirements of the organization for backups and appropriate use of storage space.

To configure a backup schedule, from the *Advanced Configuration* menu, select **Backup and Restore > Configuration** and follow these steps:

1. To enable daily, weekly, or monthly backups, use the Spacebar to enter an **X** in the appropriate field.
   For weekly or monthly backups, enter the appropriate day of the week or month as a numeral, where Monday=1.
   To disable backups, use the Spacebar to enter an **X** in the No backups field and select **OK**.
2. Enter a time for backup in the Backup Time field.
3. Select **OK**.

To perform an immediate backup, from the *Advanced Configuration* menu, select **Backup and Restore > Backup now.** When the backup confirmation displays, select **OK**.

NOTE: Before beginning a Restore operation, all VE Server services must be Running. Check Server Status. If all services are not Running, restart services. For more information, see Start or Stop VE Servers. Begin to Restore *only* when *all* services are Running.

To restore from a backup, from the *Advanced Configuration* menu, select **Backup and Restore > Restore** and select the backup file to be restored. At the confirmation screen select **Yes**.

VE reboots, and the backup is restored.

Store backups to a secure FTP server

To store backups to an FTP server, the FTP client must support SFTP on port 22.

According to backup requirements of the organization, backups can be downloaded in the following ways:

- Manually
- Through automated script
- Through the organization's approved backup solution

To download backups using the organization's backup solution, obtain detailed instructions from your backup solution vendor.

NOTE: Virtual Edition is based on Linux Debian Ubuntu x64.

Log on to VE as ddpsupport, and use the sudo command to configure your backup solution:

```
sudo <instructions from backup solution vendor>
```

Back up contents of the following folders:

/opt/dell/vsftpd/files/backup (required)

/opt/dell/vsftpd/files/certificates (strongly recommended)

/opt/dell/vsftpd/files/support (optional)

When the sudo process is complete, type **exit** and press **Enter** until the login prompt displays.

Enable Database Remote Access

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

NOTE: Dell recommends that you enable database remote access only if necessary.

1. From the *Advanced Configuration* menu, select **Database Remote Access**.
2. Use the Spacebar to enter an **X** in the Enable Database Remote Access field and select **OK**.

Enable DMZ Server Support

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

1. From the *Advanced Configuration* menu, select **Enable DMZ Server Support**.
2. Use the Spacebar to enter an **X** in the Enable DMZ Server Support field and select **OK**.

NOTE: To use Proxy Mode (DMZ Mode), you must Install and Configure Proxy Mode.

DDP Enterprise Server - VE Administrator Tasks

Set or Change DDP Enterprise Server - VE Terminal Language

It is a best practice to restart the services any time a settings change is made.

1. In the Main Menu, select **Set Language**.
2. Use the arrow keys to select the preferred language.

Check Server Status

To check the status of DDP Enterprise Server - VE Services, in the Main Menu, select **Server Status**.

The following table describes each Service and its function.

Name	Description
Dell Message Broker	Enterprise Server Bus
Dell Identity Server	Handles domain authentication requests.
Dell Compatibility Server	A Service for managing the enterprise architecture.

Name	Description
Dell Console Web Services	Supports DDP Enterprise Server - VE communication with the Dell Compatibility Server.
Dell Security Server	Provides the mechanism for controlling commands and communication with Active Directory. Used to communicate with the Dell Policy Proxy.
Dell Compliance Reporter	Provides an extensive view of the environment for auditing and compliance reporting.
Dell Core Server	A Service for managing the enterprise architecture.
Dell Inventory Server	Processes the inventory queue.
Dell Forensic Server	Provides web services for Forensic API.
Dell Policy Proxy	Provides a network-based communication path to deliver security policy updates and inventory updates.

DDP Enterprise Server - VE monitors and restarts its services, if necessary.

NOTE: If the databasecustomizer process fails, servers move to the Execution Failed state. To check the Databasecustomizer log, in the Main Menu, select View Logs.

View Logs

To check the following logs, in the Main Menu, select **View Logs**.

- System Logs

  Syslog Log
  Mail Log
  Vsftpd Log
  Auth Log (SSH)
  Postgres Log
  Monitor Log

- Server Logs

  Compatibility Server
  Console Server
  Security Server
  Message Broker
  Core Server
  Compliance Reporter
  Local Server
  Inventory Server
  Forensic Server
  Proxy Logs

- Databasecustomizer Log

Open the Command-line Interface

To open the command-line interface, in the Main Menu, select **Launch Shell**.

To exit the command-line interface, type **exit** and press **Enter**.

Generate a System Snapshot Log

To generate a System Snapshot Log for Dell Pro Support, in the Main Menu, select **Support Tools.**

1. From the *Support Tools* menu, select **Generate System Snapshot Log**.
2. At the indication that the file is created, select **OK**.

If the ddpsupport user is activated, Dell Pro Support can retrieve the log from the DDP Enterprise Server - VE SFTP server. If the ddpsupport user is not activated, contact Dell Pro Support. For more information, see Customer Support.

DDP Enterprise Server - VE Maintenance

You must remove unnecessary DDP Enterprise Server - VE backups.

If the number of backups reaches ten or available disk partition space is at ten percent or less, no more backups are stored. Existing backups are automatically removed, beginning with the oldest. If this condition occurs, you will receive an email notification that disk allocation space is low.

DDP Enterprise Server - VE Troubleshooting

If an error occurs, you will receive an email notification. Based on the information in the email notification, follow these steps:

1. Check applicable log files.
2. Restart services, as needed. It is a best practice to restart the services any time a settings change is made.
3. Generate a System Snapshot Log.
4. Contact Dell Pro Support. For more information, see Customer Support.

Post-Installation Configuration Tasks

After installation, some components of your environment may need to be configured, based on the Dell Data Protection solution used by your organization.

Configure VE for Dell Data Protection | Cloud Edition

To configure VE to support Dell Data Protection | Cloud Edition, in the VE Remote Management Console, set the Cloud Storage Protection Enabled protection policy to True.

Install and Configure EAS Management for Dell Data Protection | Mobile Edition

To use Dell Data Protection | Mobile Edition, you must install and configure EAS Management. If you do not intend to use Dell Data Protection | Mobile Edition, skip this section.

Prerequisites

- The logon account for the EAS Mailbox Manager Service must be an account with permissions to create/modify Exchange ActiveSync policy, assign policies to user mailboxes, and query information about ActiveSync devices.
- The EAS Configuration Utility must be run with Administrator permissions to modify files and restart Services.
- Network connection to the DDP Enterprise Server - VE is required.
- Have the hostname or IP address of the DDP Enterprise Server - VE available.
- Microsoft Message Queuing (MSMQ) must already be installed/configured on the server hosting the Exchange environment. If not, install MSMQ 4.0 on Windows Server 2008 or Windows Server 2008 R2 (on the server hosting the Exchange environment) – http://msdn.microsoft.com/en-us/library/aa967729.aspx

During the Deployment Process

If you intend to use Exchange ActiveSync to manage mobile devices through Dell Data Protection | Mobile Edition, your Exchange Server environment must be configured.

Install EAS Device Manager

1. In the Dell Data Protection | Mobile Edition installation media, navigate to the EAS Management folder. In the EAS Device Manager folder, copy setup.exe to your *Exchange Client Access Server(s)*.
2. Double-click **setup.exe** to begin the installation. If your environment includes more than one *Exchange Client Access Server*, run this installer on each one.
3. Select the language for installation, then click **OK**.
4. Click **Next** when the *Welcome* screen displays.
5. Read the license agreement, agree to the terms, and click **Next**.
6. Click **Next** to install EAS Device Manager in the default location of C:\Inetpub\wwwroot\Dell\EAS Device Manager\.
7. Click **Install** at the *Ready to Begin Installation* screen.

   A status window displays the installation progress.
8. If desired, check the box to show the Windows Installer log and click **Finish**.

Install EAS Mailbox Manager

1. In the Dell Data Protection | Mobile Edition installation media, navigate to the EAS Management folder. In the EAS Mailbox Manager folder, copy setup.exe to your *Exchange Mailbox Server(s)*.
2. Double-click **setup.exe** to begin the installation. If your environment includes more than one *Exchange Mailbox Server*, run this installer on each one.
3. Select the language for installation, then click **OK**.
4. Click **Next** when the *Welcome* screen displays.
5. Read the license agreement, agree to the terms, and click **Next**.
6. Click **Next** to install EAS Mailbox Manager in the default location of C:\Program Files\Dell\EAS Mailbox Manager\.
7. At the *Logon Information* screen, enter the credentials of the user account that will log on to use this Service.

   User Name: DOMAIN\Username

   Password: password associated with this user name

   Click **Next**.
8. Click **Install** at the *Ready to Begin Installation* screen.

   A status window displays the installation progress.
9. If desired, check the box to show the Windows Installer log and click **Finish**.

Use the EAS Configuration Utility

1. On the same computer, go to **Start > Dell > EAS Configuration Utility > EAS Configuration** to run the EAS Configuration Utility.
2. Click **Setup** to configure EAS Management Settings.

3 Enter the following information:

DDP Enterprise Server - VE hostname

Dell Policy Proxy Polling Interval (the default is 1 minute)

Select the box to run EAS Device Manager in report-only mode (recommended during deployment).

NOTE: The Report-only mode allows unknown devices/users to have access to Exchange ActiveSync but still reports the traffic to you. Once your deployment is up and running, you can change this setting to tighten security.

Click OK.

4 A success message displays. Click Yes to re-start IIS and EAS Mailbox Manager Services.

5 Click Quit when finished.

After the Deployment Process

Once your deployment is up and running, and you are ready to tighten security, follow the steps below.

On your Exchange Mailbox Server(s)

1 Go to Start > Dell > EAS Configuration Utility > EAS Configuration to run the EAS Configuration Utility.

2 Click Setup to configure EAS Management Settings.

3 Enter the following information:

DDP Enterprise Server - VE hostname

Dell Policy Proxy Polling Interval (the default is 1 minute)

Clear the box to run EAS Device Manager in report-only mode

Click OK.

4 A success message displays. Click Yes to restart IIS and EAS Mailbox Manager Services.

5 Click Quit when finished.

Enable Manager Trust Chain Check

If you do not intend to use Enterprise Edition for SED or Bitlocker Manager, skip this section.

By default, the Manager Trust Chain Check is turned off. To enable Manager Trust Chain Check, disable trust validation on the client computer before client activation.

To disable trust validation, set the following registry setting on the client computer:

HKLM\System\CurrentControlSet\Services\CredMgmtAgent\Parameters\DisableSSLCertTrust (DWORD (32-bit) Value) = 1

Disabling trust validation lessens security but allows you to use a self-signed certificate for pilots, POCs, etc. For a production environment, Dell recommends public CA-signed or domain-signed certificates.

VE Remote Management Console Administrator Tasks

Assign Dell Administrator Role

1 In the left pane, click Protect & Manage > Domains.

2 Click the *Members* icon of the Domain you want to add a user to.

3 Click Add Users.

4 Enter a filter to search the User Name by Common Name, Universal Principal Name, or sAMAccountName. The wild card character is *.

   A Common Name, Universal Principal Name, and sAMAccountName must be defined in the enterprise directory server for every user. If a user is a member of a Domain or Group but does not appear in the Domain or Group Members list in the Dell Remote Management Console, ensure that all three names are properly defined for the user in the enterprise directory server.

   The query will automatically search by common name, then UPN, and then sAMAccount name until a match is found.

5 Select users from the *Directory User List* to add to the Domain. Use <Shift><click> or <Ctrl><click> to select multiple users.

6 Click Add Selected.

7 Click the *Details* icon of the specified user.

8 On the top menu, select the *Admin* tab.

9 Select the administrative roles to add to this user.

10 Click Save.

Log in with Dell Administrator Role

1 Log out of the VE Remote Management Console.

2 Log in to the VE Remote Management Console with Domain user credentials.

Click "?" in the upper right corner of the VE Remote Management Console to launch the Administrator Help. The *Get Started* page displays. Follow the instructions to add a domain.

Baseline polices have been set for your organization but may need to be modified depending on your specific needs, as follows (licensing and entitlements guide all activations):

- Windows computers with Hardware Crypto Accelerators will be encrypted
- Windows computers will be encrypted
- Computers with self-encrypting drives will be encrypted
- External media will not be encrypted
- Devices connected to ports will not be encrypted
- BitLocker management is not enabled
- Cloud Edition is not enabled
- Mobile Edition is not enabled

See the Administrator Help topic "Manage Policies" to learn how to work with policies.

0 XXXXXA0 X